## APPENDIX I

EXAMPLES OF PRIMITIVE RESPONSE FUNCTIONS	
Response Mechanism	Description
:exec	Executes a shell command or script with the appropriate
	arguments filled in.
:mail	Mails a mail template using substituted arguments in the
·	mail template file to the appropriate user or
	Administrator.
:notify	Sends an on-line notification of the message template
·	with the arguments substituted for the appropriate user
	or Administrator.
:append-log	Using a format string as an argument we can make
	entries in the specified system log file. The log entry can
	possibly cause another case to fire.
:kill-process	This will kill or stop the specified process.
:disable-host	Blocks all traffic and access from a specified system that
	is passed as an argument. This may or may not involve
	controlling a router or firewall via the agent.
:disable-service	Stops or tuns off a specific network service from a specific
	host, user, or network domain. Examples of network
	services include http, mail, ftp, etc.
:disable-account	Allows disabling of a specified user or all user accounts.
	It is possible to permanently disable the account (e.g.,
	requiring manual intervention to reinstate it) or a
	temporary measure that can be automatically reinstated.
:enable-account	Allows an account that has been temporarily disabled to
	be reinstated or reactivated.
EXAMPLES OF CBR	KNOWLEDGE SHARING RESPONSE FUNCTIONS
Response Mechanism	Description
:set-sysflag	Sets a flag in the CBR agent(s) of the appropriate name
.set systag	along with a data value obtained from the current
	situation. A flag can either be set locally, or across a
	group of collaborating CBR agents. Optional arguments
	can assign a timeout to the flag. The flag will either
	disappear at a specified time, or after certain duration of
	time.
:unset-sysflag	Unsets the named flag and makes it disappear
:set-property	Allows the flag to also represent properties of key, value
	pairings. Flags and flag-properties can be used to
	represent information that can be shared between
	multiple resources and multiple CBR agents.
:unset-property	Removes the property from the flag data structure

:increment-flag	Uses a count field associated with the flag to keep track of
J	arbitrary counts or frequencies of events. An Optional
	argument can automatically decrement the flag count
	after a certain amount of time.
:decrement-flag	Decrements the flag-count either locally, or across
	multiple CBR agents
EXAMPLES OF KNOWLEDGE SHARING RESPONSE FUNCTIONS	
Response Mechanism	Description
:activate-cb	Activates the agents that monitor the resource associated
	with the case base (e.g., turns on a log file monitor).
:deactivate-cb	Disables the agent that monitors the resource associated
	with the case base. Because the agent is disabled, no
	additional events associated with that resource is
	processed by the system, and no automated responses are
	carried out.
:activate-case	Makes the named case active. An optional argument can
	specify a new timeout that specifies how long the case
	should remain active.
:deactivate-case	Makes the named case inactive, so that it will no longer
	perform any automated responses.
:add-template	Allows new additional cases to be added dynamically to
	the case base. The new case that is added uses values
	from the current situation to tailor the chosen template.